UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

LAZEMA JOHNSON on behalf of herself and all others similarly situated, *Plaintiff,* v. PERRY JOHNSON & ASSOCIATES, INC., CONCENTRA HEALTH SERVICES, INC., and SELECT MEDICAL HOLDINGS CORPORATION *Defendants.*	Case No.: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Lazema Johnson ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendants Concentra Health Services, Inc. ("Concentra"), Select Medical Holdings Corporation ("SMC") and Perry Johnson & Associates, Inc. ("PJ&A", together with Concentra and SMC: the "Defendants") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsel's investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure Plaintiff's and Class Members' personally identifiable information ("PII") and personal health information ("PHI") (collectively, "Private Information"), including but not limited to names, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses, dates and times of service, Social Security numbers, insurance information, clinical information such as laboratory and diagnostic testing results, medications, treatment facility names, and healthcare provider names, of Plaintiff and the Class members.

2. This action pertains to Defendants' unauthorized disclosure of Plaintiff's and Class Members' Private Information that occurred between in or around March 27, 2023, through May 2, 2023 (the "Data Breach").[1]

3. Defendants disclosed Plaintiff's and the other Class Members' Private Information to unauthorized persons as a direct and/or proximate result of their failure to safeguard and protect their Private Information.

4. Defendants' position as preeminent health organizations that hold a wide range of patient information means that they should have known how to prevent a data breach, and/or mitigate harm from such a breach. Defendants had a heightened duty to protect Plaintiff's and other Class Members' Private Information.

5. Defendants' security failures enabled hackers to steal the Private Information of Plaintiff and other members of the Class—defined below. These failures put Plaintiff's and Class Members' Private Information at a serious, immediate, and ongoing risk. Additionally, Defendants' failures caused costs and expenses associated with the time spent and the loss of productivity from taking time to address and attempt to ameliorate the release of personal data. Mitigating and dealing with the actual and future consequences of the Data Breach has also created a number of future consequences for Plaintiff and Class Members—including, as appropriate, reviewing records of fraudulent charges for services billed but not received, purchasing credit monitoring and identity theft protection services, the imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, the loss of property value of their Private Information, and the stress, nuisance, and aggravation of dealing with all issues resulting from the Data Breach.

[1] https://www.pjats.com/downloads/Notice.pdf (last visited March 6, 2024).

6. The Data Breach, which impacted at least 3,998,162[2] individuals, was caused, and enabled by Defendants' violation of their obligations to abide by best practices and industry standards concerning the security of patients' records and Private Information. Defendants failed to comply with security standards and allowed their patients' Private Information to be compromised, which could have been prevented or mitigated after the Data Breach occurred.

7. Accordingly, Plaintiff asserts claims for: negligence; breach of implied contract; unjust enrichment; and seeks injunctive relief, monetary damages, and statutory damages, as well as all other relief as authorized in equity or by law.

THE PARTIES

8. Plaintiff Lazema Johnson ("Ms. Johnson") is a resident of Philadelphia, Pennsylvania, and a citizen of Pennsylvania. Ms. Johnson received medical services from Concentra and received a Notice of Security Incident from PJ&A, on behalf of Concentra, on or about February 8, 2024. In order to receive medical treatment from Concentra, Ms. Johnson was required to disclose her Private Information, which was then entered into Defendants' databases and maintained by Defendants.

9. Defendant Concentra is a Nevada Corporation with its principal place of business at 5080 Spectrum Drive, Suite 1200, West Addison, TX 75001. Concentra can be served through its registered agent at: C T CORPORATION SYSTEM located at 120 South Central Avenue Clayton, MO 63105. As of September 30, 2023, Concentra operated 539 stand-alone occupational health centers and 135 onsite clinics at employer worksites throughout 41 states. Concentra delivers occupational health services, consumer health, and other direct-to-employer care in its occupational health centers, virtually through its telemedicine program, and in its onsite clinics

[2] https://www.hipaajournal.com/pja-data-breach/ (last visited March 6, 2024).

located at the workplaces of employer customers. Concentra's occupational health services include workers' compensation injury and physical rehabilitation care as well as employer services consisting of substance abuse testing, physical exams, clinical testing, and preventive care. Consumer health consists of patient-directed urgent care treatment of injuries and illnesses. Direct-to-employer services consist of the services described above as well as advanced primary care at Concentra's onsite clinics.

10. Defendant SMC is a Delaware corporation with its principal place of business located at 4714 Gettysburg Road, P.O. Box 2034 Mechanicsburg, Pennsylvania. SMC wholly owns Concentra. On the New York Secretary of State's Office, Concentra identifies its Principle Executive Office Address as being located at the same address as SMC on: 4714 Gettysburg Road, Mechanicsburg, PA, 17055. SMC has multiple locations in this District.

11. Defendant PJ&A is a Nevada corporation with its principal place of business at 755 W Big Beaver Rd #1300, Troy, MI 48084. PJ&A is a third-party service provider that provides medical transcription and reporting services. To facilitate PJ&A's services, Concentra and SMC shared the sensitive Private Information of its patients with PJ&A.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C.§ 1332(d). The amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

13. The Court has jurisdiction over PJ&A because it is a corporation headquartered in Michigan. Michigan is the physical location of many of the relevant witnesses and documents at issue, and the PJ&A servers breached in the Data Breach are located in Michigan.

14. The Court has general personal jurisdiction over Defendants Concentra and SMC because they, personally or through its agents, Defendants operate, conduct, engage in, or carry on a business or business venture in this State.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because PJ&A has its headquarters in this District, and a substantial part of the events giving rise to this action occurred in this District.

FACTUAL BACKGROUND

16. Between approximately March 27, 2023, and May 2, 2023, "An unauthorized party gained access to the PJ&A network . . . and, during that time, acquired copies of certain files from PJ&A systems.[3]

17. According to the "Cyber Incident Notice" posted on PJ&A website,[4] the PII/PHI affected in the Data Breach compromised the names, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses, dates and times of service, Social Security numbers, insurance information, clinical information such as laboratory and diagnostic testing results, medications, treatment facility names, and healthcare provider names, of Plaintiff and the Class members.

18. Upon information and belief, on November 10, 2023, Defendant Concentra was notified by Defendant PJ&A of "an event that may affect the security of information related to certain individuals, including Concentra's patients[.]"[5] Despite this notification, Defendants made

[3] https://www.pjats.com/downloads/Notice.pdf (last visited March 6, 2024).
[4] *Id.*
[5] https://www.concentra.com/about-us/notice-of-data-security-event/ (last visited March 6, 2024).

no effort to notify or otherwise warn Plaintiff and Class Members of the Data Breach until February 8, 2024.

19. On February 8, 2024, Concentra posted a page on its website noting the "event" and referring to a "Cyber Incident Notice" posted by PJ&A.[6] The Cyber Incident Notice, in turn, stated that PJ&A's network had been accessed by an "unauthorized third party . . . between March 27, 2023, and May 2, 2023[.]"[7] The PJ&A notice further stated that "[b]eginning on or around September 29, 2023," the third party "provided the results of its review to its affected customers and began working with them to notify individuals whose information was identified during the review.[8] Despite this, Defendants provided absolutely no notice to Plaintiff or the Class until January 9, 2024, more than nine months after the Data Breach and approximately two months, if not more, after Defendant Concentra learned of the Data Breach from PJ&A. Even then, despite posting a notice on its website on January 9, 2024, Concentra waited until February 8, 2024, almost an entire month, to begin sending written notice to Plaintiff and the Class.

20. On January 9, 2024, Concentra also confirmed that the protected health information of 3,998,162 patients was compromised in the PJ&A Data Breach.[9]

21. On or about February 8, 2024, Defendant PJ&A began providing notice to Plaintiff and Class Members of the Data Breach, including disclosures similar to those noted above. The Notice of Data Breach received by Plaintiff is attached hereto as **Exhibit A**.

---

[6] *Id.*
[7] https://www.pjats.com/downloads/Notice.pdf (last visited March 6, 2024).
[8] *Id.*
[9] https://www.hipaajournal.com/pja-data-breach/ (last visited March 6, 2024).

22. Concentra's Notice of Privacy Practices states, "You have the right to receive a notice that a breach has resulted in your unsecured private information being inappropriately used or disclosed. We will notify you in a timely manner if such a breach occurs."[10]

23. Despite this, notice of the Data Breach, which came more than ten months after the Data Breach, amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

24. The Data Breach occurred because Defendants failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendants failed to implement data security measures designed to prevent this attack, despite repeated public warnings to the healthcare industry about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past. Defendants did not properly contain patient health data, which requires a heightened level of protection. Defendants failed to disclose to Plaintiff and Class Members the material fact that they did not have adequate data security practices to safeguard customers' personal data, and in fact falsely represented that their security measures were sufficient to protect the Private Information in their possession.

25. Had Plaintiff known that her data would be stored with improper security measures, she would have reevaluated what information she chose to provide to Concentra, which collected and stored the data of thousands of patients or sought another provider of emergency medical services.

[10] https://www.concentra.com/-/media/project/concentra/dotcom/usa/files/hipaa/13_nop-english.pdf?rev=46e85199654d4815b8d36fb7e49646dd&t=20230807153345 (last visited March 6, 2024).

26. Defendants' failure to provide immediate formal notice of the Breach to Plaintiff and Class Members, and their delay of several months in providing notice, exacerbated the injuries resulting from the Data Breach.

27. Defendants' failure to provide immediate formal notice of the Breach to Plaintiff and Class Members, and their delay of several months in providing notice, exacerbated the injuries resulting from the Data Breach.

A. Defendants Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Patients' Private Information, Despite a Rise in Data Breaches Affecting the Healthcare Industry

28. Defendants were aware of or should have been aware of the risk of data breaches in the healthcare industry, which has had well-publicized breaches from misuse or misconfigurations over the past four years.

29. Defendants operate national healthcare services, yet Defendants did not allocate adequate resources for cybersecurity protection of patient information.

30. Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Defendants had a heightened duty to protect patient Private Information.

31. Defendants failed to ensure that proper data security safeguards were being implemented throughout the breach period.

32. Defendants failed to ensure that its healthcare operations would not be impacted in case of a data breach.

33. Defendants had obligations created by HIPAA, industry standards, common law, and representations made to Class Members to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

34. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants and any of their affiliates would comply with their obligations to keep such information confidential and secure from unauthorized access.

35. Defendants' failure to provide adequate security measures to safeguard patients' Private Information is especially egregious because Defendants operate in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to patients' highly confidential Private Information.

36. Ponemon Institute, an expert in the annual state of cybersecurity, has indicated that healthcare institutions were the top target for cyber-attacks in 2020.[11]

37. In fact, Defendants had been on notice for years that the medical industry is a prime target for scammers because of the amount of confidential patient information maintained. In 2019 alone, numerous entities in the healthcare sector suffered high-profile data breaches, including Quest Diagnostics and LabCorp.

B. Defendants' Data Security and HIPPA Violations

38. Defendants' data security lapses demonstrate that it did not honor its duties to protect patient information by failing to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protect patients' Private Information;

c. Properly maintain their own data security systems for existing intrusions;

d. Ensure that they employed reasonable data security procedures;

[11] IBM Security, Cost of a Data Breach Report, PONEMON INST. 5 (2020), https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf (last visited March 6, 2024).

e. Ensure the confidentiality and integrity of electronically maintained PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

g. Implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

h. Protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

i. Protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

j. Ensure compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or Train all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b).

C. Damages to Plaintiff and the Class

39. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

40. The information obtained by hackers and scammers is an extremely valuable commodity that is commonly traded on the black market and results in the diminishment of the value of a person's electronic presence years into the future when it is misused.

41. Plaintiff and the Class have experienced or currently face a substantial risk of out of-pocket fraud losses such as loss of funds from bank accounts, medical fraud and/or identity theft, fraudulent charges on credit cards, targeted advertising, suspicious phones calls, and similar identity theft.

42. Plaintiff and Class Members have also incurred out of pocket costs for protective measures such as credit freezes or payment for phone scam detection.

43. Plaintiff and Class Members suffered a loss of the property value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of the loss of the property value of personal information in data breach cases.

44. Class Members who paid Defendants for their services were also damaged via "benefit of the bargain" damages. Such members of the Class overpaid for a service that was intended to be accompanied by adequate data security—but was not. Part of the price Class Members paid to Defendants was intended to be used by Defendants to fund adequate data security. Defendants did not properly comply with its data security obligations. Thus, the Class Members did not get what they paid for.

45. Members of the Class have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

46. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.

47. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[12]

[12] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or

48. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, loans, or even giving false information to police during an arrest.

49. In the medical context, Private Information can be used to submit false insurance claims, obtain prescription drugs or medical devices for black-market resale, or get medical treatment in the victim's name. As a result, Plaintiff and Class Members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit and tax filings for an indefinite duration.

50. In the months and years following the Data Breach, Plaintiff and Class Members will experience a slew of harms because of Defendants' ineffective data security measures. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, targeted advertising without patient consent, and emotional distress.

51. Plaintiff values her privacy, especially in receiving medical services, and would not have paid the amount that he did for services if he had known that her information would be maintained using inadequate data security systems.

D. The Value of Privacy Protections and Private Information

52. At all relevant times, Defendants were well aware that the Private Information they collected from Plaintiff and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

53. Private Information is a valuable commodity to cyber attackers. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an

---

identification number, alien registration number, government passport number, employer or taxpayer identification number[.]"

array of crimes including identify theft, and medical and financial fraud.[13] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground websites, commonly referred to as the dark web.

54. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[14] In 2022, 1,802 data compromises were reported that impacted over 422 million victims—marking a 42% increase in the number of victims impacted since 2021.[15] That upward trend continues.

55. The ramifications of Defendants' failure to keep Plaintiff's and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

56. Further, criminals often trade stolen PII on the "cyber black- market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

57. Approximately 21 percent of victims do not realize their identities have been compromised until more than two years after it has happened. This gives data thieves ample time to seek multiple treatments under the victim's name.

---

[13] What to Know About Identify Theft, Fed. Trade Comm'n, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited March 6, 2024).

[14] Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout, CISION PR NEWSWIRE (Jan. 19, 2017) https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html (last visited March 6, 2024).

[15] 2022 Annual Data Breach Report, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited March 6, 2024)

58. Medical information is especially valuable to identity thieves. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendants knew or should have known this and strengthened their data systems accordingly, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

CLASS ACTION ALLEGATIONS

59. Plaintiff brings claims on behalf of himself, and for certain claims, on behalf of the proposed class of:

> All individuals whose PII/PHI was subjected to the Data Breach, including all individuals who were sent a notice of the Data Breach by Defendants.

60. The following people are excluded from the Class: (1) any Judge or Magistrate Judge presiding over this action and the members of their family; (2) Defendant, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current employees, officers, and directors; (3) persons who properly execute and file a timely request for exclusion from the class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel, and their experts and consultants; and (6) the legal representatives, successors, and assigns of any such excluded persons.

61. Plaintiff hereby reserves the right to amend or modify the Class definitions with greater specificity or division after having had an opportunity to conduct discovery.

62. ***Numerosity*:** The proposed Class contains members so numerous that separate joinder of each member of the class is impractical. Defendants have identified at least 3,998,162 individuals whose Private Information may have been improperly accessed and compromised in the Data Breach.

63. ***Commonality*:** There are questions of law and fact common to the proposed class. Common questions of law and fact include, without limitation:

a. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, inter alia, HIPAA;

b. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendants properly implemented their purported security measures to protect Plaintiff's and Class Members' Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendants took reasonable measures to determine the extent of the Data Breach after they first learned about it;

e. Whether Defendants disclosed Plaintiff's and Class Members' Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendants' conduct constitutes breach of an implied contract;

g. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class Members' Private Information;

h. Whether Defendant were unjustly enriched by their actions; and

i. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief or other equitable relief, and the measure of such damages and relief.

64. ***Typicality*:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of Plaintiff and Class Members are based on the same legal theories and arise from the

same unlawful and willful conduct because all had their Private Information compromised because of the Data Breach, due to Defendants' misfeasance.

65. ***Policies Generally Applicable to the Class*:** This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect the Class uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

66. ***Adequacy of Representation*:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

67. ***Superiority*:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

68. ***Predominance***: Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

69. ***Injunctive Relief***: Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

70. ***Ascertainability***: Members of the Class are ascertainable. Class Membership is defined using objective criteria, and Class Members may be readily identified through Defendants' books and records.

CLAIMS FOR RELIEF

Count I: Negligence
(On Behalf of Plaintiff and All Class Members)

71. Plaintiff restates and realleges the foregoing allegations as if fully set forth herein.

72. Upon Defendants accepting and storing the Private Information of Plaintiff and the Class on their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Private Information was private and confidential and should be protected as private and confidential.

73. Defendants owed a duty of care not to subject Plaintiff and the Class's Private Information to an unreasonable risk of exposure and theft, because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

74. Defendants owed numerous duties to Plaintiff and the Class, including the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in their possession;

b. To protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

75. Defendants also breached its duty to Plaintiff and Class Members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendants failed to provide adequate supervision and oversight of the Private Information with which they were and are entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class Members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

76. Defendants knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches within the medical industry.

77. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' Private Information.

78. Defendants breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

79. Because Defendants knew that a breach of their systems would damage thousands of their customers, including Plaintiff and Class Members, Defendants had a duty to adequately protect their data systems and the Private Information contained thereon.

80. Defendants' duty of care to use reasonable security measures arose because of the special relationship that existed between Defendants and their patients, which is recognized by laws and regulations including but not limited to HIPAA and common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

81. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

82. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

83. Defendants' duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

84. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information. Defendants' misconduct included failing to: (1) secure Plaintiff's and Class Members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

85. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of Defendants' networks and systems;

c. Allowing unauthorized access to Class Members' Private Information; and

d. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

86. Through Defendants' acts and omissions described in this Complaint, including their failure to provide adequate security and their failure to protect Plaintiff's and Class Members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure

Plaintiff's and Class Members' Private Information during the time it was within Defendants' possession or control.

87. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to, failing to adequately protect the Private Information, and failing to provide Plaintiff and Class Members with timely notice that their sensitive Private Information had been compromised.

88. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

89. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class Members suffered damages as alleged above.

90. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, inter alia, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class Members.

Count II: Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

91. Plaintiff restates and realleges the foregoing allegations as if fully set forth herein.

92. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of healthcare and data administration services, as well as implied contracts for the implementation of data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

93. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with Concentra when they first entered into contracts with Concentra to receive medical services.

94. The valid and enforceable implied contracts to provide medical services that Concentra entered into with Plaintiff and Class Members include Defendants' promise to protect nonpublic Private Information given to Defendants or that Defendants created on their own from disclosure.

95. When Plaintiff and Class Members provided their Private Information to Concentra in exchange for medical services, they entered into implied contracts pursuant to which Concentra, and subsequently PJ&A, agreed to reasonably protect such Private Information.

96. Concentra solicited and invited Class Members to provide their Private Information as part of Concentra's regular business practices. Plaintiff and Class Members accepted Concentra's offer and provided their Private Information to Concentra. This Private Information was later maintained by or under the control of Defendants, who assumed the obligation to secure and protect it.

97. Plaintiff and Class Members have fully performed their obligations under these contracts.

98. By entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

99. Class Members who paid money to Defendant reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

100. Under these implied contracts, Defendant were obligated to: (a) provide medical services to Plaintiff and Class Members; and (b) protect Plaintiff and Class Members' Private

Information provided to obtain the benefits of such services. In exchange, Plaintiff and members of the Class agreed to pay money for these services, and to turn over their Private Information.

101. Both the provision of medical services and the protection of Plaintiff and Class Members' Private Information were material aspects of these implied contracts.

102. The implied contracts for the provision of medical services include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Information, which are also acknowledged, memorialized, and embodied in multiple documents (including, among other documents, Defendants' Data Breach notification letter).

103. Consumers of medical services value their privacy, the privacy of their dependents, and the ability to keep confidential their Private Information associated with obtaining such services. Plaintiff and Class Members would not have entrusted their Private Information to Defendants and entered into these implied contracts with Defendants without an understanding that their Private Information would be safeguarded and protected; nor would they have entrusted their Private Information to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

104. A meeting of the minds occurred as Plaintiff and Class Members agreed and provided their Private Information to Defendants and paid for the provided services in exchange for, among other things, both the provision of healthcare and the protection of their Private Information.

105. Plaintiff and Class Members performed their obligations under the contract when they paid for Defendants' services and/or provided Defendants with their Private Information.

106. Defendants materially breached their contractual obligation to protect the nonpublic Private Information Defendants gathered when the Private Information was accessed and exfiltrated through the Data Breach.

107. Defendants materially breached the terms of these implied contracts. Defendants did not maintain the privacy of Plaintiff and Class Members' Private Information as evidenced by their notifications of the Data Breach to Plaintiff and Class Members. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA or HIPAA, or otherwise protect Plaintiff and Class Members' private information as set forth above.

108. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

109. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in the value between the healthcare with data security protection they paid for and the healthcare they received.

110. Had Defendants disclosed that their data security was inadequate or that they did not adhere to industry-standard security measures, neither the Plaintiff, Class Members, nor any reasonable person would have gone to Defendants to obtain healthcare services.

111. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of

their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses to mitigate the effects of the Data Breach, including time lost responding to the Breach, and the loss of the benefit of the bargain they struck with Defendant.

112. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

113. Plaintiff and Class Members are also entitled to injunctive relief requiring defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

Count III: Unjust Enrichment
(On Behalf of Plaintiff and All Class Members)

114. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

115. Plaintiff brings this claim in the alternative to her breach of implied contract claim.

116. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendants and provided Defendants with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and should have been entitled to have Defendants protect their Private Information with adequate data security.

117. Defendants knew that Plaintiff and Class Members conferred a benefit on Defendants and have accepted or retained that benefit. Defendants profited from Plaintiff's purchases and used Plaintiff's and Class Members' Private Information for business purposes.

118. Defendants failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff and Class Members for the value that their Private Information provided.

119. Defendants acquired the Private Information through inequitable means as it failed to disclose the inadequate security practices previously alleged.

120. If Plaintiff and Class Members knew that Defendants would not secure their Private Information using adequate security, they would have made alternative healthcare choices that excluded Defendant.

121. Plaintiff and Class Members have no adequate remedy at law.

122. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred on them.

123. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendants and that the Court grants the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures; requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

ix. requiring Defendants to conduct regular database scanning and securing checks;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for

all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect himself;

xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorney's fees and costs, and any other expenses, including expert witness fees;

G. Pre-and-post judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is hereby demanded for all claims so triable.

Dated: March 6, 2024

Respectfully submitted,

FINK BRESSACK

/s/ *David H. Fink*
David H. Fink (P28235)
Nathan J. Fink (P75185)
38500 Woodward Ave, Suite 350
Bloomfield Hills, MI 48304
Telephone: (248) 971-2500
dfink@finkbressack.com
nfink@finkbressack.com

Alan M. Feldman, Esq.*
Zachary Arbitman, Esq.*
Samuel Mukiibi, Esq.*
FELDMAN SHEPHERD WOHLGELERNTER TANNER WEINSTOCK & DODIG, LLP
1845 Walnut Street, 21st Floor
Philadelphia, PA 19103
T: (215) 567-8300
F: (215) 567-8333
afeldman@feldmanshepherd.com
zarbitman@feldmanshepherd.com
smukiibi@feldmanshepherd.com

Kevin C. Harp, Esq. *
O'CONNOR & PARTNERS, PLLC
255 Wall Street
Kingston, New York 12401
T: (845) 303-8777
F: (845) 303-8666
KHarp@onplaw.com

Application for admission to be submitted